Inf Syst Front
DOI 10.1007/s10796-014-9538-x

A security-and quality-aware system architecture for Internet of Things

Sabrina Sicari · Cinzia Cappiello · Francesco De Pellegrini · Daniele Miorandi · Alberto Coen-Porisini

Abstract Internet of Things (IoT) is characterized, at the system level, by high diversity with respect to enabling technologies and supported services. IoT also assumes to deal with a huge amount of heterogeneous data generated by devices, transmitted by the underpinning infrastructure and processed to support value-added services. In order to provide users with valuable output, the IoT architecture should guarantee the suitability and trustworthiness of the processed data. This is a major requirement of such systems in order to guarantee robustness and reliability at the service level. In this paper, we introduce a novel IoT architecture able to support security, privacy and data quality guarantees, thereby effectively boosting the diffusion of IoT services.

Keywords Internet of Things · Security · Privacy · Data quality · System architecture

S. Sicari · A. Coen-Porisini
Dipartimento di Scienze Teoriche e Applicate, Università degli studi dell'Insubria, via Mazzini, 5, Varese 21100, Italy

S. Sicari
e-mail: sabrina.sicari@uninsubria.it

A. Coen-Porisini
e-mail: alberto.coenporisini@uninsubria.it

C. Cappiello (✉)
Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Piazza Leonardo da Vinci 32, Milan 20133, Italy
e-mail: cinzia.cappiello@polimi.it

F. De Pellegrini · D. Miorandi
CREATE-NET, via alla Cascata, 56/D Povo, Trento 38123, Italy

F. De Pellegrini
e-mail: francesco.depellegrini@create-net.org

D. Miorandi
e-mail: daniele.miorandi@create-net.org

D. Miorandi
e-mail: daniele.miorandi@u-hopper.com

D. Miorandi
U-Hopper, P.za Manci 17 Povo, Trento 38123, Italy

Published online: 04 November 2014

1 Introduction

The term "Internet of Things" (IoT) describes a broad aggregate of technologies and research disciplines that enable the Internet to reach out into the world of physical objects. However there are (at least) two main interpretations of what IoT means and therefore what kind of technologies should be taken into account (Miorandi et al. 2012). On the one hand, IoT is often associated with technologies such as RFIDs, short-range wireless communications, real-time localization and sensor networks. In this perspective, the main ingredient is represented by the use of pervasive sensors communication and embedded devices. On the other hand, there is a specific research line arguing that the meaning of the term "thing" should not be confined to a physical object but comprises also abstract (virtual) components, and in particular services.

In our work we try to move forward from this dichotomy and we aim to merge such contrasting visions. Hence, despite a lot of technical work is still required in order to make a system as a whole from the two separated souls of the IoT, namely the sensing part and the service part. The main objective of our work is to introduce a lightweight data management and service framework: the system model that we propose is hence meant to handle large amount of data coming from heterogeneous technologies, as those encompassed by customary IoT scenarios.

In this paper we present the design of a reference system architecture whose aim is to overcome the following key issues that are incumbent technical bottlenecks in the state of art:

- *Data extraction* – Most of the existing approaches address the issue of extracting data from heterogeneous sources but very few focus on the analysis of the quality and the provenance of data sources. Evaluating the trustworthiness of incoming data is a key step in order to assess the quality of the information obtained by integrating and processing them.
- *Integration* – Existing IoT enabling technologies (RFIDs, WSNs, etc.) are currently treated as separated entities, and are not fully integrated. Full integration is indeed a very important requirement in order to enable efficient in-network processing of data and decision-making.
- *Standardized design* – Lack of a standardized approach to system design hinders portability and ease of design. In fact, services making use of IoT data are typically built in an ad-hoc and centralized way, limiting the potential offered by the presence of a large number of embedded devices equipped with sensing, identification, communication and computing capabilities.
- *Reconfigurability* – The existing IoT deployments are hardly reconfigurable; they are conceived for very specific applications, for which "vertical" silos-based systems are defined. A reconfigurable system, based on open standards would allow one to achieve scale economies, facilitating the widespread adoption of IoT-based technologies.

Addressing such issues at the system architecture level will lead to systems that encompass several novel functionalities, including:

- The possibility to handle environmental and contextual data acquired through different technologies (e.g., RFID, sensors) in a unified manner;
- A novel data representation model, specifically tailored to IoT scenarios, enabling the creation of a distributed database that would allow different intelligent networked objects, called NOS (NetwOrked Smart objects) to access data from heterogeneous sources in a unified and transparent way;
- A set of lightweight methods for the creation and maintenance of a NOS layer and for performing data discovery and query;
- A NOS-tailored lightweight service framework able to support dynamic reconfiguration and self-capabilities;
- A set of mechanisms for remote orchestration of NOS-executed services in an Internet/Intranet setting;
- Implementation of the aforementioned concepts in a suitable middleware platform;
- A set of security and privacy mechanisms able to ensure data confidentiality, data integrity and anonymity in a distributed setting;
- A set of modules that through the analysis of data values and provenance provide indications about data quality dimensions such as timeliness, completeness accuracy and source trustworthiness

In particular, this article mainly focuses on the last two issues, which are related to the data that the system should manage. We believe that management of the incoming data is the most critical task for the usage and success of the IoT infrastructure. Therefore, we start from the analysis of security and Data Quality (DQ) issues in order to define the system requirements to satisfy. On the basis of such an investigation an architecture that considers all these aspects is proposed. Furthermore, the present work aims to provide guidelines for the design of NOS objects able to deal with security and quality issues.

The paper is organized as follows. Section 2 presents a reference scenario, Section 3 explains in details the security and data quality needs in the IoT context, while Section 4 introduces the system architecture. Section 5 applies our solution to an application case study. Section 6 presents a short overview of the related state of the art and the main motivations that support the work highlighting its potential impact. Finally, Section 7 ends the paper and provides hints for future work.

2 Reference scenario

In this section we present a sample scenario based upon the concept of smart retailing experience (Kourouthanassis et al. 2007). The scenario targets advanced shopping applications, in which the user is guided through a store and can interact (directly or through its IoT-enabled smartphone) with physical objects and digital services. One of the problems faced by managers of retailing stores, indeed, is that they have no direct access to knowledge on the behaviour of users within their store. Indeed, it is easy to track the number of people entering the store: also, advanced business analytics solutions are readily available for understanding the purchasing behaviour of customers. However, the time interval between the time a customer enters the store and the moment it reaches the check-out counter is still out of reach.

The scenario (summarized in Fig. 1) includes the following entities (i) a shopping cart, embedding an active tag for localization purposes (ii) a number of locators, fixed devices used for tracking in real-time the movement of carts and users in the store (iii) a smartphone, equipped with proximity technologies such as Bluetooth, ZigBee and/or NFC and connected to the Internet through either WiFi or 3G (iv) physical products that

Fig. 1 Store case study

can be purchased within the store and are equipped with a transceiver that turns them into active, smart objects. The actors present in the scenario are: (i) the user, which enters the shop to buy products (ii) the store manager, who wants to maximize the effectiveness of its point-of-sale.

In our scenario, a user getting into the shop would collect a shopping cart and start visiting the store. The shopping cart is equipped with an active tag, which communicates with the locators. Bluetooth low-power or ZigBee technologies can be used for this purpose. The signals from the tags are processed by the locators and sent, via an appropriate data management infrastructure, to the cloud hosting the service. The store manager can access in real-time advanced analytics about the behaviour of customers within her point-of-sale. By analysing the patterns of movement of users within the point of sale and by assessing how changes in the layout and/or the presence of specific promotions/sales change the movement pattern, the store manager can optimize the positioning of goods within the store and maximize the effectiveness of promotional campaigns. Similarly, the store management processes can be optimised, so that, e.g., the system recognizes in real time that a queue is building up at the checkout counters and hence additional staff should be moved there to increase capacity.

The tag is also able to associate with the user smartphone, using the same wireless technology it uses for positioning purpose. The smartphone runs an app, through which the user can be presented with contents, ads and personalized discount that are location-aware (i.e., they are relevant given the fact that the user is in proximity of a given good). Examples include advertising specific promotions/sales on-going, suggestion of goods based on the purchasing history of the customer and so on so forth. Furthermore, the smartphone can communicate directly with smart objects, so that, e.g., information about the whole product chain and product lifecycle can be retrieved. In the case of, e.g., food retailing store, such information can include the production date/place and the whole list of steps along the food transformation and logistic chains. In the case of, e.g., clothes, information can relate to the production process, the materials used and/or reviews from fashion magazines. In the paper, we will show how the proposed architecture fits the described scenario by effectively leveraging information about the quality and security of accessed data.

3 IoT: Security and data quality needs

In the IoT, physical and virtual objects interact and communicate exchanging information about the environment and the context they are situated in. In such a scenario, the heterogeneity of technology and processed data requires standardization and the definition of services that are able to query the different data objects and retrieve the information that the users need in an easy and safe way. In order to effectively address these challenges, it is necessary to consider security, privacy and data quality issues. The former ones need to be considered because IoT services should allow users to gather and exploit all the required data avoiding any risks to their security and privacy (Sicari et al. 2012). The latter one allows users to access high quality trusted data, which in turn improve the correctness and effectiveness of their decision-making processes.

3.1 Security and privacy issues

The huge amount of data handled in IoT context poses new open research challenges on the security and privacy topics. In fact, the diffusion of IoT services is conditioned by the capability to provide a good level of security preserving at the same time the user private life. Such goals are reached through the guarantee of authentication, data confidentiality, data integrity and anonymity levels.

Authentication represents the need to identify the user or the object which are authorized to access the data by means some mechanisms (more or less robust), such as password, digital signature, challenge and response and so on.

Data confidentiality represents the need to allow the access to data only to authorized entities, by means the adoption of various encryption scheme, such as RSA. Data integrity represents the need to guarantee the original data content from unauthorized changes. Notice that in IoT context the entities may be users, objects or NOS. For example looking at the defined reference scenario only the store manager, after an authentication phase, is authorized to access the information related to his/ her customer habits for marketing purposes and it is fundamental to prevent data from any malicious change, maybe performed by the somebody paid by a competitor.

The main point is to find solutions for handling in a secure manner the identity of NOS and the related authorization processes. Although the management of user identity well investigated in the literature, the management of NOS identities raises a number of novel issues to deal with. Looking at the state-of-the art, a starting point could be represented by the concept of federation (Bhargav-Spantzel et al. 2007), thanks to which one can distinguish between the different identity attributes to be assigned to NOS or users. In our framework, in fact, not only users, but also authorized objects, NOS, may access data. This requires addressing two important aspects: first, the definition of an access control mechanism, and second, the definition of an object authentication process (with a related identity management system).

Also, privacy issues represent another fundamental IoT research challenge. A privacy policy defines the way in which data referring to individuals can be collected, processed and diffused according to the rights that individuals are entitled to (Sicari et al. 2012), (Directive 95/46/EC of the European Parliament).

Depending on the specified purpose, a certain level of anonymity may be guaranteed. The anonymity represents the absence of identifiable data of a user or of data that allows inferring identifiable data (e.g., first name, surname etc.). For example, from the customer's point of view it is important to guarantee his/her privacy. In fact by mining shopping user behaviour it may be possible to retrieve sensitive data such as religious or ethical preferences. For example, a customer who only buys vegetables and never buys meat might be vegan. In order to avoid the violation of the user privacy a key role is played by the correct definition of privacy policies and the related defined confidentiality and anonymous level of information.

The main reason that makes privacy a fundamental IoT requirement lies in the envisioned IoT-aided application domains. Various frameworks have been proposed in order to account for privacy issues in the system design phase, such as Kaos (van Lamsweerde and Letier 2000), NFR (L. Chung et al. 1993; Mylopoulos et al. 1992), GBRAM (Anton 1996), PRIS (Kalloniatis et al. 2008), DYDAP (Sicari et al. 2012). The development of implementations in our context would benefit from the definition of a general model, able to represent all IoT fundamental entities and their relationships, and to take into account the requirements of scalability, dynamic environment, and data stream access control.

Summarizing in order to develop a secure service in IoT-aided environment, due to the vast amount of data and related sources, a crucial point is the definition of methods able to assess the level of security and privacy of the incoming heterogeneous data, providing a fine level of granularity. This requires the definition of a score method and to store some ad hoc metadata in order to choose the data, which are suitable for satisfying services requirements. Such needs are addressed in this work.

3.2 Data quality issues

IoT seems to be the next frontier for innovation, competition and productivity (Manyika et al. 2011). The volume of data and the variety of the sources lead to new challenges in the data quality field in which researchers and practitioners aim to evaluate the "fitness for use" of data sets (Wang and Strong 1996). Traditional data quality approaches mainly focused, among the others, on the following activities: (i) definition and assessment of dimensions able to evaluate the fitness of specific structured or semi-structured data for an intended use, (ii) object identification to evaluate whether data in the same source or in different ones represent the same object in the real world (Batini and Scannapieco 2006); (iii) definition of improvement methods (e.g., data cleaning, process analysis for detection of poor data quality root causes). Most of the methods and techniques proposed are based on two main assumptions: data are structured and the purposes for which data are used are known. Clearly, these two assumptions are not valid in the IoT environment in which heterogeneous sources are available and the data are not related to a predefined set of processes but they can be used to satisfy different requirements. In such a scenario, new assessment techniques have to be proposed and additional data quality dimensions have to be defined. In particular, some efforts should be directed toward the evaluation of the value of the data that is affected by both intrinsic dimensions and by dimensions related to the data provenance such as the credibility and reputation of the data sources.

As regards the former category of dimensions, they describe the gathered values. In particular, we consider only the dimensions that can be automatically evaluated: accuracy, completeness, and timeliness. *Accuracy* can be defined as the extent to which data are correct: data

values stored in the database correspond to real-world values (Wang and Strong 1996; Ballou and Pazer 1985). Such a dimension is associated with a score in the interval [0,1] that reveals the proximity of the values to the correct ones.

Completeness is defined as the degree to which a given data collection includes data describing the corresponding set of real-world objects. It is also associated with a score in the range [0,1] that indicates the percentage of data fields that are associated with a proper value. Finally, we consider the *timeliness* dimension: it is defined as the extent to which the age of data is appropriate for the task at hand. The temporal validity of the used data is defined by two components: age and volatility. Age or currency is a measure of how old the information is, based on how long ago it was recorded. Volatility is a measure of information instability, the frequency of change of the value for an entity attribute (Bovee et al. 2001).

Finally, in this paper, the concept of *trust* is undoubtedly associated with the concept of source reputation and thus reliability: trust can be defined as the probability by which data are suitable to be included in a specific process providing value.

Such quality dimensions are fundamental for some application fields. For example, in the considered application scenario the manager, when accessing the real-time advanced analytics, should be aware of the quality of the retrieved information in order to take most effective decisions. For example, s/he should be aware that occurred problems in the data gathering caused the presence of missing values in the data set and then the information provided by the system refers to a partial view about the customers' behaviour. On the other hand, the product information available for the customers of the store should be enriched with data quality and security information in order to provide information about the degree of trustworthiness. This is an important aspect, especially for the food products for which showing the list of the ingredients or nutritional information is extremely helpful for people that have intolerances or cannot eat some products for religious or ethical issues. The source used to gather the displayed information can influence the data reliability: information extracted from the web has a degree of trustworthiness in general lower than the information provided by a certified source.

Looking at these examples, it is already possible to understand the importance of enriching the processed data with information about their quality and thus the importance of the definition and collection of metadata.

Also data integration is a relevant issue in the IoT. In order to support data fusion, data quality plays a fundamental role addressing issues related to object identification (also for identity management). Note that data fusion can be also driven by the assessment of the value of data that might be used, together with other techniques, to manage the data volume. In fact, the value of data might be a support for the selection of the suitable sources that can satisfy a specific request.

4 System architecture

In order to satisfy both security and data quality issues we define a system architecture that is sketched in Fig. 2. Data coming from the environment and/or context are acquired through a distributed interface composed of a (potentially) large number of simple, inexpensive, embedded nodes, named *e-Nodes*.

E-Nodes refer to nodes that provide data generated automatically, named *System Data*, and nodes that provide data generated by humans, named *Human Data*. Examples of the former ones are RFIDs, smart tags, simple sensors, traditional databases and so on. Social networks belong to the latter category. Clearly, the set of e-Nodes represents a heterogeneous environment. In fact, data provided by such e-Nodes can be extremely diverse and also the communication with them might require different communication technologies. E-Nodes' operations are driven by a set of computationally powerful smart nodes NOS (NetwOrked Smart Object). Each NOS is characterized by a structure divided into three layers, *Analysis*, *Data Annotation* and *Integration*. Each layer performs a specific set of actions, as described in next section. The goal of NOSs is to acquire raw data coming from e-Nodes and process them, according to the *Analysis* and *Data Annotation* phases, as shown in Fig. 2, in order to provide in output a specific representation of the gathered information, called *IoT Data*. The output information is represented according to a well-specified syntax and includes a semantic description of the data content. Once that data have been normalized, they can be integrated in order to satisfy the users' requests, according to the rules defined at *Integration layer*. Users interact with the system by using some specific services that can be either atomic or composite. The former services simply provide users with the access to one source; while the latter ones integrate information gathered by multiple sources and allow users to access data by using advanced queries.

In the following sections we provide details about the three layers, i.e., *Analysis*, *Data Annotation* and *Integration* that let users and applications easily access data acquired by e-Nodes.

4.1 Analysis

The data collected by the different e-Nodes has to be processed in order to support a specific application to use and understand them. In the *Analysis* phase, data are analysed to

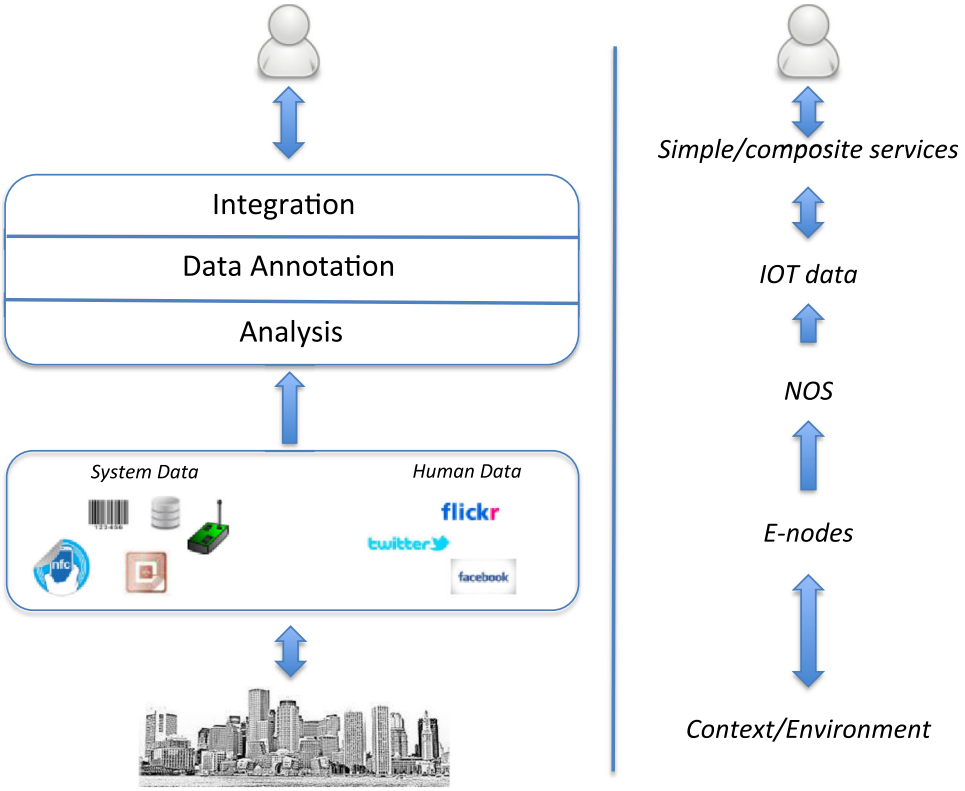

Fig. 2 The System Architecture

support the subsequent phases. In particular, we assume that we access data with their description and that for each incoming data it is possible to extract the following information:

- *Data source*: the data sources are heterogeneous and are classified in *System Data* and *Human Data* as previously described.
- *Data communication mode*: the way in which data are collected, e.g., discrete vs. streaming communication.
- *Data schema*: the type (e.g., text vs. numbers vs. multimedia), the format and the metric of the data attributes (if available and if needed – on the basis of the context) are specified.
- *Security metadata*: specify the nature of data (sensitive or not) and which security properties are guaranteed. In particular, security metadata provide details about confidentiality, authentication, integrity and privacy.
- *DQ metadata*: provide information about the quality level of the data and the related sources. Data trustworthiness can be measured in terms of timeliness (that depends on the data volatility and currency), data completeness, data accuracy, source reputation and data provenance (data is created by the source or in other cases the source provides a processed version – system data vs. human data).

Clearly some of such metadata may not be available if a source is unknown or not registered. In this case the fields are left empty. Correspondingly, this will prevent NOSs to assess the data quality provided.

The task of the *Analysis layer* is to evaluate whether the input data satisfy all the defined requirements, such as security and quality requirements. In fact, data should provide both a suitable security level (e.g., encrypted data) and quality level for the considered scenario; in some other cases, some actions for guaranteeing the customer satisfaction have to be performed. At this layer, by considering all the input information, it must be possible to gather side information useful to verify, for example, the data encryption, the existence of a certification authority, the data anonymity, the need for authentication or the suitability of data for a specific task.

In details, in order to retrieve all the security features, the *Analysis* phase consists of a set of functionalities to assess the security level:

1. Check the data source.
2. Access the information required to authenticate the source and to decrypt the data, if the data source is a registered one. For registered sources, the system maintains indeed complete knowledge, including, e.g., encryption scheme, keys used etc. Some registered sources may use neither authentication credentials nor encryption. Further, for unregistered/unknown sources no information may be available.
3. Perform authentication of the source (if registered).

4. Decrypt information (if encrypted).
5. Access the data type.
6. A score is assigned to: authentication level; confidentiality level; integrity level and privacy level. The score range is in [0–1]. More in details, if the authentication is based, for example, on digital signature the score is set to 1, if the authentication string is NULL the score is set to 0; while, for example if the authentication is based on a short password the score is set to 0.2.

A similar approach is adopted for evaluating integrity and confidentiality levels. Scores are assigned according to the robustness of the used encryption technique and of the adopted key distribution schema.

A similar approach is used for privacy requirements. For example, if the identity of the source (i.e., id sensor node, in case of system data, or nick name, in case of human data) is not revealed the privacy level should be set to 1. In general the definition and the adoption of a privacy model and the related privacy policies are associated to a high score. In general the system administrator, according to required security and quality requirement, defines the score assignment rules.

The *Analysis* layer further evaluates the quality of the incoming data. This is based on the following steps:

1. Access the information about the data source
2. The source is evaluated on the basis of its reputation. Source reputation can be defined as the sum of two main factors: the content and the owner reputation. The former depends on the number of times the source fails to provide a good answer to a user request (if feedback is available) while the latter depends on the history of the organization (or person) that owns the data.
3. Looking at the source we are also able to retrieve important information about the data provenance. It is important to store if the analysed data have been just created or updated or they are just copied from other systems.
4. Look at the source content and analyse the type of the stored information.
5. A score is assigned to: timeliness, completeness and accuracy. Timeliness, i.e., temporal validity is calculated on the basis of the freshness of data (it is retrieved by looking at the last update) and on the frequency of changes: data is still valid if the time interval between the analysis time and the last update is less than the average interval between two updates. As regards, completeness and accuracy, they are calculated on the basis of algorithms that depend on the data type and communication mode.

For all the analysed dimensions the score is in the range [0–1].

In summary, the output of the *Analysis* layer is a description record with the following information: data source, data schema and security and DQ scores.

4.2 Data annotation

The data sources are heterogeneous and in order to handle such different data have to be accurately described, as shown in Fig. 3. *Data Annotation* layer receives the information from the *Analysis* layer and provides a description of the data by adding a set of metadata. More formally, data are annotated with a sequence of metadata containing the following information:

1. *Data Source*: *a reference to the source is provided*
2. *DataType*: *describes the type of data*
3. *Data Values*
4. *Security metadata*: *describe the security aspects providing the values associated with*:
   i. *Authentication*
   ii. *Confidentiality*
   iii. *Integrity*
   iv. *Privacy*
5. *DQ metadata*: *describe the level of data quality aspects providing the values associated with*:
   i. *Timeliness*
   ii. *Completeness*
   iii. *Accuracy*
   iv. *Source reputation*

The output of this phase is the annotation of data with appropriate metadata. Note that the choice to provide a score for each security and DQ requirements is due in order to make a solution flexible for smart integration in different application scenarios. In fact, a solution in which there are only general security and quality scores, without details about all the different security and DQ dimensions, does not allow the system to precisely identify weaknesses and strengths of the different input data sources. For example, there exist application scenarios in which it is required to use data that have a high level of integrity and confidentiality, but there is not of interest to satisfy privacy requirement.

4.3 Integration

After the annotation process the data may be integrated according to the application needs. Such an operation is performed at the *Integration* layer. In fact, it is possible to compare and merge data coming from different technologies, in order to better satisfy user requests. The functionalities offered at the *Integration* layer depend on the specific application domain. Such a layer exploits the information about security and quality level offered by the *Data Annotation* layer. It does so in order to support a smart integration process. More in details, the *Integration* layer is aware of the characteristics of

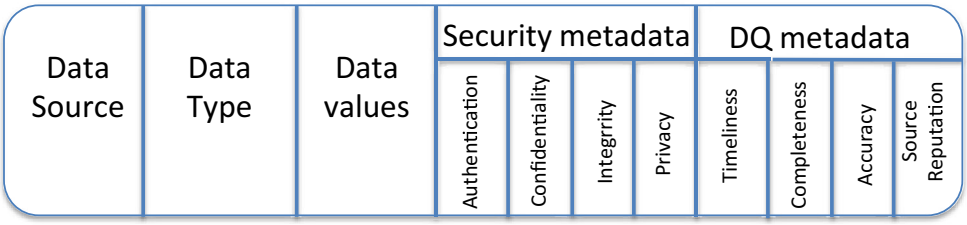

Fig. 3 Data annotation schema

the sources and related data and metadata and such information could be used for two different purposes: *knowledge* level and/or *operating level*. The former refers to the possibility to provide the integrated information annotated with the security and data quality scores in order to let the users be aware of data trustworthiness. The latter refers to some integration procedures, which might be affected by the data provided by different levels. For example, security and data quality levels can be used for the selection of sources (if there are alternatives) to be integrated. For example, if the application domain aims at providing a service characterized by error-free data and high confidentiality scores, the integration level should select sources which are able to satisfy these requirements.

Such a feature of our framework makes it suitable for adoption in different contexts.

Summarizing, the final goal of the NOS layer is used to enable the access to IoT data through a properly engineered lightweight data discovery mechanism. NOSs communicate with e-Nodes by means of different short-range wireless communication techniques (e.g., NFC, UWB, IEEE802.15.×, Bluetooth). NOSs can run atomic services, which can make use of IoT data residing on different NOSs. The NOS layer can be connected to IP-based networks (Internet, Intranet), enabling nodes/users to access the set of offered services in a standardized way. The set of services available on NOSs can be dynamically reconfigured from a network administrator through an Internet connection with the NOS overlay. The atomic services offered by the NOSs can be orchestrated by a remote server to offer composite servers to the end-users through standard Web services approaches, exploiting the potentiality of the *Integration* layer.

As NOSs include self-organising features, they can be deployed where and when needed; through their interface with enterprise platforms and IoT enabling technologies, they can be used to enrich software platforms, making them able to interact in a standardised way with the physical world.

5 Application case study

For better explaining the proposed architecture, let us consider Julia, a frequent customer of the Store, presented in Section 2 that registered to use the app provided to support her in shopping. The registration phase is the first step in which security can be seen as a crucial issue. In fact, in order to better support the customer during shopping, personal information is required. Information like name and phone number is classified as identifiable data, while age and spoken language are classified as generic data since they can be used for statistical purposes only. Julia also specifies her preferences about the products available in the store. She can specify allergies and ingredients/materials that she does not want to include in her shopping for religious/ethical reasons. For example, for clothing, she can specify the preference to wear only natural materials excluding all synthetic fibers.

Inputs from customers are only one of the sources that the system analyses. As previously described the other inputs are data about the customer' behaviour retrieved from the different active tags and locators available in the shop and products data gathered from external sources. In fact, we assume that information about the products is collected by the platform in different ways. It can be extracted automatically by traceability systems, it can be provided by the suppliers or it can be gathered from alternative sources (e.g., web).

In the system proposed in this paper and depicted in Section 4, all these sources are first analysed in order to define the details about data contained and the quality and security levels. As regards quality, each source can be characterized by a reputation index that describes the trustworthiness of each content and that in *Data Annotation* phase will be added to the other quality metadata that can be assessed accessing to the retrieved values. As regard security, during *Analysis* phase after the authentication of the source, the information, if required, is decrypted and the data type is accessed. A score is assigned to each security metadata in order to assess, authentication confidentiality, integrity and privacy level. During *Data Annotation* phase the assessed security score will be added in the field named *Security metadata* and used for evaluating the source data.

The data integration operation will be performed on the basis of the functionalities that the system supports. If the manager has to perform analysis to better place the products on the shelves, an integration of locators, active tags and products data has to be performed. In a situation where Julia stops in front of a specific cloth, the application will integrate products 'data with her requirements and will inform her about the materials the specific product is made of. In both

cases, the integration is designed to consider data quality and security levels and to calculate the aggregate data quality and security index. Such an index makes Julia aware of the degree of confidence by which the provided data can be relied on, while preserving her privacy.

6 Related work

This section aims to compare the previous contributions with the approach proposed in this paper. In particular, in Section 6.1 we presents the main contributions to the IOT literature and in Section 6.2 we describe the specific approaches so far proposed to include security and data quality aspects.

6.1 Main contributions in the IoT literature

Internet of Things is a vision of future technological ubiquity. The diffusion of the IoT paradigm would allow for the implementation and the diffusion of really innovative services, in several applications fields. The most crucial challenge in building such a system lies in the lack of common software framework, i.e., there is a clear lack of a solution to let the software populating different environments combine and build larger composite systems in a seamless fashion.

In order to fill this gap, the scientific community has started several interesting research initiatives that have proposed innovative solutions. For example, in recent years, the availability of web service solutions has provided a real framework able to allow one system to leverage the services of another one according to the principles of Service Oriented Architectures. Service-oriented Communications (SOC) technologies manage web services by creating a virtual network and adapting applications to the specific needs of users rather than users being forced to adapt to the available functionality of applications. Furthermore, such architecture does not require the modules of a system to be isomorphic. Actually, the service centric environment composed by the services is naturally open, platform independent, flexible and adaptable (Papazoglou et al. 2007; Yu et al. 2008). Therefore such features make SOC/SOA suitable to build first the software, then the service infrastructure of Internet of things. Towards the adoption of SoA paradigm in the IoT domain another crucial point is represented by the possibility to exploit the research results that have been provided in the last ten years. In fact, using standardized and well-defined solutions the take-off process of specific IoT solutions will become easier. Exploiting the potentiality and solutions provided by web service technology a flexible, dynamic and open platform of services will be provided to Internet of things.

Although the decision of adopting SoA architecture in Internet of Things is shared by the majority of scientific community, at the moment the state of the art in this area is mostly limited to starting research activities. More specifically, a solution, PeerTrack,[1] proposes to apply SOC in order to realize scalable and Internet-based RFID traceability networks. The approach uses P2P, Web-service-based architecture guaranteeing scalability for large-scale applications such as those encompassed by the Internet of Things scenario. Although the idea is interesting, it also poses several challenges; for instance, questions about which data models to employ and which service design on query processing to adopt, are still waiting for a final answer. Another solution, PERCI (PERvasiveServiCe Interaction),[2] is based on the composition of independent services, which should be provided to the user in a consistent and seamless way. The goal of that work is to investigate and develop new methods for mobile interactions with the Internet of Things. In fact, by using Semantic Web service technologies there is a concrete mean to overcome the semantic incompatibility between different services. Moreover, describing services semantically it is possible to automatically generate a uniform user interface dealing with all the proposed semantic user interface annotations. Such user interfaces, in particular, could be optimized to provide easier and more familiar interactions with physical objects in the Internet of things and the services associated with them. But, there is still no consistent way to integrate web services and means for physical interaction: from an architectural point of view several technical requirements have to be met, such as modelling, composition and provisioning of Semantic Web services.

Several related scenarios have been encompassed in related EU projects, especially with respect to the services part. For example, the FP7 COMPOSE (Collaborative Open Market to Place Objects at your Service)[3] project aims to design and develop an open marketplace, in which data from Internet-connected objects can be easily published, shared, and integrated into services and applications. The marketplace will provide a number of key technological enablers, organized into a coherent framework covering aspects related to management of objects, integration and service delivery. The basic concept underpinning the COMPOSE approach is to treat smart objects as services, which can be managed using standard service-oriented computing approaches and can be dynamically composed to provide value-added applications to end users. The end results of the project shall be a vertical marketplace ecosystem for Internet of Things, able to become a sort of global store for Internet-connected objects and their data.

The iCORE project (iCORE)[4] is a flagship European project on Internet-of-Things. It aims at empowering the IoT with cognitive technologies and is focused around the concept of

[1] http://cs.adelaide.edu.au/peertrack/
[2] http://www.hcilab.org/projects/perci/index.htm
[3] http://www.compose-project.eu/
[4] http://www.iot-icore.eu/

virtual objects (VOs). VOs are semantically enriched virtual representation of the capabilities/resources provided by real-world objects. Through the inception of VOs it becomes possible to easily re-use Internet-connected objects through different applications/services, also supporting their aggregation into more composite services (composite virtual objects – CVOs). VOs provide a unified representation for smart objects, hiding from the application/service developers low-level technological details as well as any underlying technological heterogeneity. VOs provide a standardized way to access objects' capabilities and resources. One key element in the iCORE project is the use of advanced cognitive techniques for managing and composing VOs in order to improve IoT applications and better match user/stakeholder requirements. Application scenarios considered include ambient assisted living, smart office, transportation and supply chain management.

A dynamic architecture for services orchestration and self adaptation has been proposed in IoT.EST, (Internet of Things Environment for Service Creation and Testing).[5] The project defines a dynamic service creation environment that gathers and exploits data and information from sensors and actuators that use different communication technologies/formats. Such an architecture deals with different issues such as composition, of business services based on re-usable IoT service components, automated configuration and testing of services for "things", abstraction of the heterogeneity of underlying technologies to ensure interoperability.

Furthermore, focusing on semantic web services, the Ebbits project[6] designed a SOA platform based on open protocols and middleware, effectively transforming every subsystem or device into a web service with semantic resolution. The goal is to allow businesses to semantically integrate the Internet of Things into mainstream enterprise systems and support interoperable end-to-end business applications.

Finally, dealing with security, privacy and trust issue there are uTRUSTit project[7] and Butler.[8] The former one is a project integrating the user directly in the trust chain, guaranteeing transparency in the underlying security and reliability properties of the Internet of Things. If successful, uTRUSTit shall enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgments on the trustworthiness of such systems. Butler aims to allow users to manage their distributed profile allowing data duplication and identities control over distributed applications. The final purpose is to implement a framework able to integrate user dynamic data (i.e., location, behaviour) in privacy and security protocols.

[5] http://ict-iotest.eu/iotest/
[6] http://www.ebbits-project.eu/
[7] http://www.utrustit.eu
[8] http://www.iot-butler.eu

In the presented approach, besides identifying the best suited software solution, another challenge is the integration of heterogeneous data and technologies. In order to achieve such a goal we propose to focus the architectural design onto:

- A modular architecture for the seamless and incremental integration of IoT-enabled services in standard software-based systems;
- An open architecture for the inclusion of heterogeneous IoT-enabling technologies (including RFID, sensors etc.) into Internet-based software systems.

This system architecture should support the definition of:

– A set of self-* methods for the distributed and autonomic management and run-time optimization of the platform;
– A set of secure and privacy-aware mechanisms and their integration in the proposed platform;
– A set of DQ assessment methods that can be used for different types of data and in different scenarios.

It is important that the quest for an open architecture is pushed by most of the above research initiatives since it has the potential to enable innovative SMEs to develop a wide spectrum of novel services leveraging such a platform to bridge the digital and physical worlds.

At the lower level, the open platform would create also brand new markets for RFIDs, smart card producers and sensors, fostering the growth of an industrial sector key to the economy of the next decades.

The major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications (Atzori et al. 2010).

6.2 Security and data quality issues in IoT

It is clear that in order to guarantee a real diffusion of IoT paradigm three key requirements are to be addressed: security, privacy and data quality.

The satisfaction of a required security and privacy level means to guarantee *confidentiality*, *integrity* and *anonymity* requirements.

Concerning data confidentiality, Role-Based Access Control (RBAC) is a consolidated approach, which well matches the features of IoT environments (Sandhu et al. 1996). The main advantage of RBAC, in an IoT perspective, is the fact that access rights can be modified dynamically by changing the role assignments. The IoT context requires the introduction of new forms of RBAC-style solutions, in particular, considering that IoT data will likely represent streams to be accessed in real-time, rather than being stored in static

databases. The literature offers few proposals, which are classified into two main categories: those aiming to ensure authenticity, confidentiality, and integrity of data streams during transmission (Papadopoulos et al. 2007; Ali et al. 2004), and those related to access control (Lindner et al. 2006; Nehme et al. 2008). As far as data stream access control is considered, it is only recently that mechanisms to guard against unauthorized access to streaming data have been investigated.

The work in (Lindner et al. 2006) proposes a model for extending RBAC to protect data streams from unauthorized access, but there are many issues that are yet to be solved. As regards privacy, in the literature only few works address such an issue in the IoT context. In (Evans and Eyers 2012) is proposed a data tagging for managing privacy in IoT. Data representing physical phenomena or related to individuals are tagged with their privacy properties. Tagging within resource-constrained sensors raises several issues due to the expensive computation. A well-investigated solution is based on the k-anonymity. For example, in (Huang et al. 2012) is presented an access control protocol where the privacy is controlled by the users themselves. Context aware k-anonymity privacy policies and filters are designed and privacy protection mechanisms are investigated, in which users can control which of their personal data is being collected and accessed, who is collecting and accessing such data, and when these are happening. In addition, (Cao et al. 2011) presents CASTLE (Continuously Anonymizing STreaming data via adaptive cLustEring). It is a cluster-based scheme which ensures anonymity, freshness and delay constraints on data streams, since most of the existing privacy preserving techniques (i.e., k-anonymity) are designed for static data sets and not for continuous, unbounded and transient streaming data. (Cao et al. 2011) models k-anonymity on data streams and defines k-anonymized clusters, which exploit quasi-identifier attributes to determine a metric space, such that tuples can be considered points in this space. (Wang and Wen 2011) analyses the privacy risk that occurs when a Static Domain Name (DNS) is assigned to a specified IoT terminal smart device. In such a work the authors propose a privacy protection enhanced DNS scheme for smart devices, which can authenticate the original users identity and reject illegal accesses. The scheme is compatible with widely used DNS and DNSSEC protocol. In (Alcaide et al. 2013) privacy and access control mechanisms are considered together. The authors present a fully decentralized anonymous authentication protocol aimed at implementing privacy preserving IoT applications. Such a proposal is based on a credential system, which defines two roles for the participant nodes: Users, which are the nodes originating the data and Data Collectors, which are the entities responsible for the collection of data only from authorized Users; Users can anonymously authenticate themselves in front of Data Collectors proving the ownership of a valid Anonymous Access Credential (AAC) encoding a particular set of attributes. Such a system relies on no central organization: the parameters required by the system are generated in a cooperative and not central way.

Note that at present, a limited number of solutions are available, even though their computational requirements are rather high. In fact the Internet of Things is meant to connect a large number of communication and information systems. These systems will be part of everyday life in the same way mobile phones have become part of our lives. The information security properties of the IoT are hence going to become rather difficult to understand for end users, because they are hidden in pervasive systems and small devices manufactured by a large number of vendors. Trustworthiness, security functions and privacy implications are vast, and must be assessable to users and consumers. Many open issues have to be addressed in order to develop effective IoT secure services. First, the definition of globally accepted certification authorities should be addressed, together with a number of requirements that an IoT-compliant certification authority should respect.

As regards data quality, several literature contributions recognize it as one important issue to address in the IoT research field. In (Guo et al. 2013), authors claim the need of control over data sources to ensure their validity, information accuracy and credibility. Data accuracy is also one the aspect on which the authors of (Metzger et al. 2012) focus on. They observe that the presence of many data sources raises the need to understand the quality of that data. In particular, they state that the data quality dimensions to consider are accuracy, timeliness and the trustworthiness of the data provider. The huge number of data sources is considered as positive for data fusion and for the extraction and provisioning of advanced services. Besides temporal aspects (i.e., currency) and data validity, a related work adds another important dimension such as availability (Li et al. 2012), with focus on pervasive environments. Authors defined new metrics for the cited quality dimensions in the IoT environment and evaluate the quality of the real-world data available on an open IoT platform called Cosm. They have showed that data quality problems are frequent and they should be solved or at least users should be aware of the poor quality of the used data sources.

Anyway, no literature contributions propose an architecture able to manage security, privacy and data quality aspects in the IoT environment as we have proposed in this work.

7 Conclusions

Security and data quality requirements play a fundamental role to enable the widespread diffusion and take-up of the IoT paradigm. In this paper, a novel architecture, suitable for satisfying the security and data quality requirements was

introduced. Moreover, the adoption of such an architecture would provide an annotated IoT data representation, security, privacy and quality aware, able to satisfy users' and domain-specific needs.

The next steps include the release of an open platform for the integration of heterogeneous IoT technologies in Web-based IT systems, including a modular and self-organizing architecture and a secure and privacy-preserving middleware. Another relevant research direction is the design of an open, standardized representation of IoT-specific data, including provenance and metadata representation for the support of semantic queries. Finally, an experimental demonstration, based on a real-world case study with real users should be conducted in order to validate the usefulness of our contribution.

Acknowledgments The work of D. Miorandi leading to these results has received funding from PAT within the framework of the LOCOS project.

References

Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). "Anonymous authentication for privacy-preserving IOT target-driven applications." *Computers & Security, 37*, 111–123.

Ali, M., Eltabakh, M., & Nita-rotaru, C. (2004). "Robust security mechanisms for data streams systems," Purdue university, csd technical report 04-019.

Anton, A. (1996). "Goal-based requirements analysis," in Proceedings of the Second International Conference on Requirements Engineering, pp. 136–144.

Atzori, L., Iera, A., & Morabito, G. (2010). "The internet of things: A survey." *Computer networks, 54*(15), 2787–2805.

Ballou, D. P., & Pazer, H. L. (1985). Modeling Data and Process Quality in Multi-input, Multi-output Information Systems. *Management Science, 31*(2), 150–162.

Batini, C., Scannapieco, M. "Data quality: concepts, methodologies and techniques." Data-Centric Systems and Applications, Springer 2006.

Bhargav-Spantzel, A., Squicciarini, A., and Bertino, E. "Trust negotiation in identity management," Security Privacy, IEEE, vol. 5, no. 2, pp. 55 –63, march-April 2007.

Bovee, M., Srivastava, R. P., & Mak, B. (2001). "A Conceptual Framework and Belief-Function Approach to Assessing Overall Information Quality." Proc. 6th Int. Conf. on Information Quality (ICIQ-2001), MA, USA, pp.311–32

Cao, J., Carminati, B., Ferrari, E., & Tan, K. (2011). "Castle: Continuously anonymizing data streams." *IEEE Transactions on Dependable and Secure Computing, 8*(3), 337–352.

Chung, L. (1993). "Dealing with security requirements during the development of information systems," in Advanced Information Systems Engineering, ser. Lecture Notes in Computer Science, C. Rolland, F. Bodart, and C. Cauvet, Eds. Springer

Evans, D., & Eyers, D. (2012). "Efficient data tagging for managing privacy in the internet of things." In Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CP- SCom 2012, Besancon, pp 244–248.

Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou X. (2013). "Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things". *Journal of Network and Computer Applications, 36*(6), 1531–1539. doi:10.1016/j.jnca.2012.12.028

Huang, X., Fu, R., Chen, B., Zhang, T., Roscoe, A. (2012). "User interactive internet of things privacy preserved access control." In 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, London, United Kingdom, pp. 597–602.

Internet of ThingsStrategicResearchRoadmap; available online at: http://ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: the PriS method. *Requirements Engineering, 13*(3), 241–255.

Kourouthanassis, P. E., Giaglis, G. M., & Vrechopoulos, A. P. (2007). Enhancing user experiencethroughpervasive information systems: The case of pervasiveretailing. *International Journal of Information Management, 27*(5), 319–335.

Li, F., Nastic, S., & Dustdar, S. (2012). Data Quality Observation in Pervasive Environments. In *Proceedings of the 2012 I.E. 15th International Conference on Computational Science and Engineering* (CSE '12). IEEE Computer Society, Washington, DC, USA, 602–609. doi:10.1109/ICCSE.2012.88

Lindner, W., & Meier, J. "Securing the borealis data stream engine," in Proceedings of the 10th International Database Engineering and Applications Symposium, ser. IDEAS'06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 137–147. [Online]. Available: http://dx.doi.org/10.1109/IDEAS.2006.40

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers A. "Big data: The next frontier for innovation, competition, and productivity" Report McKinsey Global Institute 2011. [Online] Available: http://www.mckinsey.com/mgi/publications/big_data/

Metzger, A.; Chi-Hung Chi; Engel, Y.; Marconi, A., "Research challenges on online service quality prediction for proactive adaptation," *Software Services and Systems Research – Results and Challenges (S-Cube), 2012 Workshop on European*, vol., no., pp.51,57, 5–5 June 2012 doi:10.1109/S-Cube.2012.6225512

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Survey internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.

Mylopoulos, J., Chung, L., and Nixon, B. "Representing and using non-functional requirements: a process-oriented approach," Software Engineering, IEEE Transactions on, vol. 18, no. 6, pp. 483 –497, Jun. 1992

Nehme, R., Rundensteiner, E., & Bertino, E. "A security punctuation framework for enforcing access control on streaming data," in Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on, April 2008, pp. 406 –415

Papadopoulos, S., Yang, Y., & Papadias, D. "Cads: continuous authentication on data streams," in Proceedings of the 33rd international conference on Very large data bases, ser. VLDB'07. VLDB Endowment, 2007, pp. 135–146. [Online]. Available: http://dl.acm.org/citation.cfm?id=1325851.1325870

Papazoglou, M. P., Traverso, P., Dustdar, S., & Leymann, F. (2007). Service-Oriented Computing: State of the Art and Research Challenges. *IEEE Computer, 40*(11), 38–45.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L. and Youman, C. E. "Role-based access control models," Computer, vol. 29, no. 2, pp. 38–47, Feb. 1996. [Online]. Available: http://dx.doi.org/10.1109/2.485845

Sicari, S., Grieco, L. A., Boggia, G., & Coen-Porisini, A. (2012). DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks. *Journal of Systems and Software, 85*(1), 152–166.

van Lamsweerde, A., & Letier, E. (2000). Handling obstacles in goal-oriented requirements engineering. *IEEE Transactions on Software Engineering, 26*(10), 978–1005.

Wang, R., & Strong, D. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems; Armonk; Spring, 12*(4), 5–33.

Wang, Y., & Wen, Q. (2011). "A privacy enhanced dns scheme for the internet of things." IET International Conference on Communication Technology and Application, ICCTA, Beijing, pp. 699–702.

Yu, Q., Bouguettaya, A., & Medjahed, B. (2008). Deploying and Managing Web Services: Issues, Solutions, and Directions. *The VLDB Journal, 17*(3), 537–572.

Sabrina Sicari is Assistant Professor at Universita' degli Studi dell'Insubria (Italy). She received her master degree in Electronical Engineering in 2002 and her Ph.D. in Computer and Telecommunications Engineering in 2006 from Universita' degli Studi di Catania (Italy). From September 2004 to March 2006 she has been a research scholar at Politecnico di Milano. Since May 2006 she works at Universita' degli Studi dell'Insubria in the software engineering group. Her research interests are on wireless sensor networks (WSN), risk assessment methodology and privacy models. She is a member of the Editorial Board of Computer Network (Elsevier). She is the general co-chair of S-Cube'09, a steering Committee member of S-Cube'10, S-Cube'11, S-Cube'13 and S-Cube'14, guest editor for the ACM Monet Special Issue, named "Sensor, system and Software" and AD Hoc Special Issue on Security, Privacy and Trust Management in Internet of Things era (SePriT), TPC member and reviewer for many journals and conferences.

Cinzia Cappiello is Assistant Professor in computer engineering at the Politecnico di Milano (Italy) from which she holds a Ph.D. in Information Technology (2005). Her research interests regard data and information quality aspects in service-based and Web applications, Web services, sensor data management, and Green IT. On such topics, she published papers in international journals and conferences. Cinzia is Associate Editor of the ACM Journal of Data and Information Quality. She has been co-chair of the workshops "Quality in Databases" in conjuction with VLDB 2010, "Data and Information Quality" in conjuction with CAiSE 2005, "Quality in Web Engineering" in conjuction with ICWE 2010-2013, and of the tracks "Information Quality Management in Innovative IS" of MCIS 2012 and "Data and Information quality" of ECIS 2008.

Francesco De Pellegrini (CREATE-NET) received the Ph.D. degree in 2004 in Telecommunication Engineering from the University of Padova. He is currently a senior researcher at CN and his role is Area Head of the iNSPIRE group. He has served as lecturer at the university of Trento for the master degree course of Wireless Networks. His technical research interests are location detection, multirate systems,routing, wireless mesh networks, VoIP, Ad Hoc and Delay TolerantNetworks. From the scientific standpoint, his interests are algorithms on graphs, stochastic control of networks and game theory. F. De Pellegrini has been a TPC member several internationalnetworking conferences and journals. He served as TPC Chair and of ICST Mobiquitous. Francesco has been General Co-Chair for the 2012 edition of IEEE NetGCoop, and TPC Chair for the 2014 edition. He has acted as Project Manager for the industry-funded LOCOS, CO2 and InfraNet projects. He coordinates the FET EU Project CONGAS, on the Dynamics and COevolution in Multi-Level Strategic INteraction GAmeS.

Daniele Miorandi is lead scientist within the iNSPIRE Area at CREATE-NET and Executive Vice President for R&D at U-Hopper, Italy. He received a PhD in Communications Engineering from Univ. of Padova, Italy, in 2005. His current research interests include modelling and performance analysis of large-scale networked systems, ICT platforms for socio-technical systems and distributed optimisation for smart grids. Dr. Miorandi has co-authored more than 120 papers in internationally refereed journals and conferences. He serves on the Steering Committee of various international events (WiOpt, Autonomics, ValueTools), for some of which he was a co-founder (Autonomics and ValueTools). He also serves on the TPC of leading conferences in the networking and computing fields. He is a member of ACM, ISOC and ICST.

Alberto Coen Porisini received his Dr. Eng. degree and Ph.D in Computer Engineering from Politecnico di Milano (Italy) in 1987 and 1992, respectively. He is Professor of Software Engineering at Universita' degli Studi dell'Insubria (Italy) since 2001, Dean of the the School of Science from 2006 and Dean of the Universita' degli Studi dell'Insubria since 2012. Prior to that he was Associated Professor at Universita' degli Studi di Lecce (1998-2001), Assistant Professor at Politecnico di Milano (1993-2001) and Visiting Researcher with the Computer Security Group at University of California, Santa Barbara (1992-1993). His main research interests are in the field of specification and design of real-time systems, privacy models and wireless sensor networks.